(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-362245
(P2004-362245A)
(43)公開日　平成16年12月24日(2004.12.24)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 12/14	G06F 12/14	320C	5B017
G06F 1/00	G06F 1/00	370E	5B035
G06F 15/00	G06F 15/00	330F	5B085
G06K 19/10	H04L 9/00	673D	5J104
H04L 9/32	H04L 9/00	673E	

審査請求 未請求　請求項の数 5　ＯＬ　（全 11 頁）　最終頁に続く

(21)出願番号　特願2003-159643(P2003-159643)
(22)出願日　平成15年6月4日(2003.6.4)

（特許庁注：以下のものは登録商標）
Ｂｌｕｅｔｏｏｔｈ

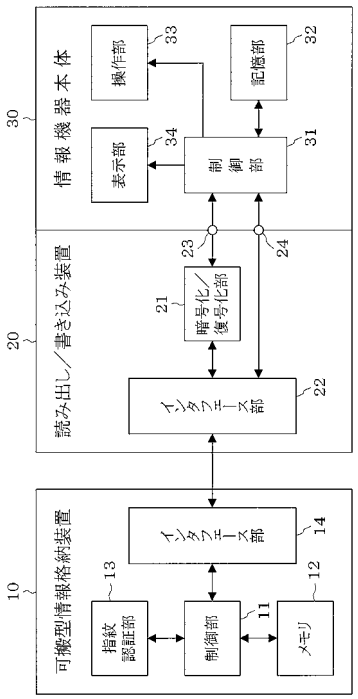
(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(74)代理人　100064621
弁理士　山川　政樹
(74)代理人　100067138
弁理士　黒川　弘朗
(74)代理人　100098394
弁理士　山川　茂樹
(72)発明者　山口　正泰
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

Ｆターム(参考)　5B017 BA05　BA07　CA14
5B035 AA14　BB09　BC01　CA38

最終頁に続く

(54)【発明の名称】個人情報入出力システム、個人情報格納装置および個人情報入出力方法

(57)【要約】
【課題】安全かつ確実に個人情報を保持し、目的の情報機器に対してその個人情報を入出力できるようにする。
【解決手段】可搬型個人情報格納装置１０に、ユーザから取得した指紋データと予め登録されている指紋データとが一致した場合にユーザを登録者本人であると認証する指紋認証部１３を設け、この指紋認証部１３により登録者本人であると認証されたときに、メモリ１２からの個人情報の読み出しまたはメモリ１２への個人情報の書き込みが行われるようにする。これにより、ユーザが指紋データの登録者でない場合には、ユーザから取得した指紋データと登録指紋データとが一致せず、ユーザが登録者本人であるとは認証されないので、メモリ１２に対する個人情報の読み出しまたは書き込みは行われない。
【選択図】　図１



【特許請求の範囲】
【請求項１】
個人情報を保持する記憶手段を備えた可搬型の個人情報格納装置と、情報機器本体に接続されかつ前記個人情報格納装置の前記記憶手段から読み出した個人情報を前記情報機器本体に出力するとともに前記情報機器本体から入力された個人情報を前記個人情報格納手段の前記記憶手段へ書き込む読み出し／書き込み装置とからなる個人情報入出力システムにおいて、
前記個人情報格納装置に設けられ、ユーザから取得した生体情報と予め登録されている生体情報とが一致した場合に前記ユーザを登録者本人であると認証する認証手段と、
この認証手段により登録者本人であると認証されたときに、前記記憶手段からの前記個人情報の読み出しまたは前記記憶手段への前記個人情報の書き込みを行う制御手段と
を備えたことを特徴とする個人情報入出力システム。
【請求項２】
請求項１に記載された個人情報入出力システムにおいて、
前記読み出し／書き込み装置は、
前記個人情報格納装置の前記記憶手段に書き込まれる前記個人情報を暗号化する暗号化手段と、
前記個人情報格納装置の前記記憶手段から読み出された暗号化された前記個人情報を復号化する復号化手段と
を備えたことを特徴とする個人情報入出力システム。
【請求項３】
個人情報を保持する記憶手段と、この記憶手段から読み出された個人情報を外部装置へ出力するとともに前記記憶手段に書き込まれる個人情報を外部装置から入力するインタフェース手段とを備えた可搬型の個人情報格納装置において、
ユーザから取得した生体情報と予め登録されている生体情報とが一致した場合に前記ユーザを登録者本人であると認証する認証手段を備え、
この認証手段により登録者本人であると認証されたときに、前記記憶手段からの前記個人情報の読み出しまたは前記記憶手段への前記個人情報の書き込みが行われることを特徴とする個人情報格納装置。
【請求項４】
可搬型の個人情報格納装置から個人情報を情報機器本体に読み出し、情報機器本体から個人情報を前記個人情報格納装置に書き込む個人情報入出力方法において、
前記個人情報格納装置で、ユーザから取得した生体情報と予め登録されている生体情報とを照合する第１のステップと、
照合の結果、２つの生体情報が一致した場合に、前記ユーザを登録者本人であると認証する第２のステップと、
前記ユーザが登録者本人であると認証されると、前記個人情報格納装置に対して前記個人情報の読み出しまたは書き込みを行う第３のステップと
を備えたことを特徴とする個人情報入出力方法。
【請求項５】
請求項４に記載された個人情報入出力方法において、
前記第３のステップは、
前記個人情報を暗号化してから前記個人情報格納装置に書き込むステップと、
前記個人情報格納装置から読み出された暗号化されている前記個人情報を復号化するステップと
を含むことを特徴とする個人情報入出力方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、個人情報入出力システムに関し、より詳しくは、可搬型の個人情報格納装置を

用いる個人情報入出力システムに関する。
また、本発明は、個人情報格納装置に関し、より詳しくは、可搬型の個人情報格納装置に関する。
本発明は、個人情報入出方法に関し、より詳しくは、可搬型の個人情報格納装置を用いる個人情報入出力方法に関する。
【０００２】
【従来の技術】
近年、個人情報が格納されたＩＣカードを携帯し、駅の改札や社員食堂などにおいてＩＣカードから支払機に個人情報を転送して電子決済を行う機会が増えている。また、個人の電子ファイルを可搬型フラッシュメモリ内に格納し、このメモリを出張先のパソコンなどに接続して電子ファイルを利用することも日常的になってきた。このように、ＩＣカードや可搬型フラッシュメモリなどの可搬型情報格納装置に個人情報やその関連情報を格納して携帯する方法は、ＩＴ社会において個人情報等を持ち運ぶ一般的な方法になりつつある（例えば、特許文献１を参照。）。
【０００３】
【特許文献１】
特開２００２－２２９８６１号公報
【０００４】
【発明が解決しようとする課題】
しかし、従来の可搬型情報格納装置には、その装置を使用する者がその装置の所有者本人かどうかを識別する機能がない。例えば、ＩＣカード型定期券では、所有者本人かどうかを識別することは不可能である。このため、万一、所有者が可搬型個人情報格納装置を紛失してしまうと、その装置を手に入れた他人が所有者になりすまし、容易に悪用することができるという問題があった。
【０００５】
本発明はこのような課題を解決するためになされたものであり、その目的は、安全かつ確実に個人情報を保持し、目的の情報機器に対してその個人情報を入出力できる個人情報入出力システムおよび個人情報格納装置を提供することにある。
【０００６】
【課題を解決するための手段】
このような目的を達成するために、本発明の個人情報入出力システムは、個人情報を保持する記憶手段を備えた可搬型の個人情報格納装置と、情報機器本体に接続されかつ個人情報格納装置の記憶手段から読み出した個人情報を情報機器本体に出力するとともに情報機器本体から入力された個人情報を個人情報格納手段の記憶手段へ書き込む読み出し／書き込み装置とからなり、個人情報格納装置に設けられかつユーザから取得した生体情報と予め登録されている生体情報とが一致した場合にユーザを登録者本人であると認証する認証手段と、この認証手段により登録者本人であると認証されたときに記憶手段からの個人情報の読み出しまたは記憶手段への個人情報の書き込みを行う制御手段とを備えたことを特徴とする。
このシステムにおいては、ユーザが生体情報の登録者でない場合には、ユーザから取得した生体情報と登録生体情報とが一致せず、ユーザが登録者本人であるとは認証されないので、記憶手段に対する個人情報の読み出しまたは書き込みは行われない。
【０００７】
また、読み出し／書き込み装置が、個人情報格納装置の記憶手段に書き込まれる個人情報を暗号化する暗号化手段と、個人情報格納装置の記憶手段から読み出された暗号化された個人情報を復号化する復号化手段とを備えるようにしてもよい。記憶手段に書き込まれる個人情報を暗号化手段で暗号化することにより、たとえ個人情報格納装置が盗まれたとしても、記憶手段の内容が読み取られる可能性が小さくなる。
【０００８】
また、本発明の個人情報格納装置は、個人情報を保持する記憶手段と、この記憶手段から

読み出された個人情報を外部装置へ出力するとともに記憶手段に書き込まれる個人情報を外部装置から入力するインタフェース手段と、ユーザから取得した生体情報と予め登録されている生体情報とが一致した場合にユーザを登録者本人であると認証する認証手段とを備え、この認証手段により登録者本人であると認証されたときに、記憶手段からの個人情報の読み出しまたは記憶手段への個人情報の書き込みが行われることを特徴とする。
この装置においては、ユーザが生体情報の登録者でない場合には、ユーザから取得した生体情報と登録生体情報とが一致せず、ユーザが登録者本人であるとは認証されないので、記憶手段に対する個人情報の読み出しまたは書き込みは行われない。

【０００９】

また、本発明の個人情報入出力方法は、可搬型の個人情報格納装置で、ユーザから取得した生体情報と予め登録されている生体情報とを照合する第１のステップと、照合の結果、２つの生体情報が一致した場合に、ユーザを登録者本人であると認証する第２のステップと、ユーザが登録者本人であると認証されると、個人情報格納装置に対して個人情報の読み出しまたは書き込みを行う第３のステップとを備えたことを特徴とする。
この方法においては、ユーザが生体情報の登録者でない場合には、ユーザから取得した生体情報と登録生体情報とが一致せず、ユーザが登録者本人であるとは認証されないので、個人情報格納装置に対する個人情報の読み出しまたは書き込みは行われない。

【００１０】

また、第３のステップは、個人情報を暗号化してから個人情報格納装置に書き込むステップと、個人情報格納装置から読み出された暗号化されている個人情報を復号化するステップとを含むようにしてもよい。個人情報格納装置に書き込まれる個人情報を暗号化することにより、たとえ個人情報格納装置が盗まれたとしても、格納されている個人情報が読み取られる可能性が小さくなる。

【００１１】

【発明の実施の形態】

以下、本発明の一実施の形態について、図面を参照して詳細に説明する。
図１は、本発明の一実施の形態に係る個人情報入出力システムの全体構成を示すブロック図である。この個人情報入出力システムは、パソコンなどの情報機器本体３０と、情報機器本体３０に接続されて使用される読み出し／書き込み装置２０と、ＩＣカードや可搬型フラッシュメモリなどの可搬型個人情報格納装置１０とから構成される。

【００１２】

可搬型個人情報格納装置１０は、装置内の各部の動作を制御する制御部１１と、個人情報を保持するメモリ（記憶手段）１２と、ユーザから取得した指紋データを基にそのユーザが登録者本人であることの認証を行う指紋認証部１３と、読み出し／書き込み装置２０との間で信号の送受信を行うインタフェース部１４とを有している。ここで、「ユーザ」とは可搬型個人情報格納装置１０を現に使用しようとする者をいい、「登録者」とは可搬型個人情報格納装置１０に予め自己の指紋を登録した者をいう。なお、可搬型個人情報格納装置１０には、電源として電池が内蔵されていてもよい。

【００１３】

読み出し／書き込み装置２０は、個人情報を暗号化するとともに暗号化された個人情報を復号化する暗号化／復号化部２１と、可搬型個人情報格納装置１０との間で信号の送受信を行うインタフェース部２２とを有している。

【００１４】

情報機器本体３０は、機器内の各部の動作を制御する制御部３１と、制御部３１を動作させるための制御プログラムや個人情報などを保持する記憶部３２と、ユーザが操作を行うための操作部３３と、各種情報を表示する表示部３４とを有している。情報機器本体３０と読み出し／書き込み装置２０との間では、入出力ポート２３を介して個人情報の送受信が行われ、制御ポート２４を介して制御信号の送受信が行われる。

【００１５】

図２は、可搬型個人情報格納装置１０の指紋認証部１３の構成を示すブロック図である。

指紋認証部１３は、ユーザの指紋を読み取り指紋データを取得する指紋センサ１３Ａと、登録者の指紋データ（以下、登録指紋データという）を保持するメモリ１３Ｂと、ユーザの指紋データと登録指紋データとを照合する照合回路１３Ｃとから構成される。指紋センサ１３Ａの一例としては、約１５０μｍ間隔でマトリクス状に複数配置され指紋の凹凸により容量が変化する容量素子と、容量素子に形成される容量を検出する複数の容量検出回路と、すべての容量検出回路によって検出された容量を濃淡に変換して画像データを生成する処理回路とからなるものがある。処理回路により生成された画像データを指紋データと呼んでいる。照合回路１３Ｃにおいては、画像のパターンマッチング技術を利用して指紋データを照合する。照合の結果、ユーザの指紋データと登録指紋データとが一致すると、ユーザが登録者本人であると認証される。

【００１６】

図３は、可搬型個人情報格納装置１０の外観を示す図である。指紋認証部１３の指紋センサ１３Ａは可搬型個人情報格納装置１０のケース１５の表面に設けられている。指紋センサ１３Ａの位置は、図４に示すようにユーザが可搬型個人情報格納装置１０を手に持って情報機器（情報機器本体３０に読み出し／書き込み装置２０が接続されたもの）に接続しようとしたときに、ユーザの指が触れやすい位置にするとよい。これにより、ユーザが可搬型個人情報格納装置１０を使用する際に、指紋センサ１３Ａがユーザの指紋を確実に読み取ることができる。指紋センサ１３Ａを除く可搬型個人情報格納装置１０の他の構成要素は、ケース１５の内部に収容されている。

【００１７】

次に、本実施の形態に係る個人情報入出力システムの動作について説明する。

まず、事前に可搬型個人情報格納装置１０に指紋データを登録するときの動作について、図５を参照して説明する。

可搬型個人情報格納装置１０のコネクタ１６を、情報機器本体３０に接続された読み出し／書き込み装置２０のコネクタ（図示せず）に差し込む。これにより、可搬型個人情報格納装置１０と読み出し／書き込み装置２０とが電気的に接続されると（ステップＳ１，ＹＥＳ）、読み出し／書き込み装置２０から可搬型個人情報格納装置１０へ電力が供給される（可搬型個人情報格納装置１０に電池が内蔵されている場合には、読み出し／書き込み装置２０からの電力供給は不要。以下同様）。

【００１８】

自己の指紋を可搬型個人情報格納装置１０に登録しようとする者は、可搬型個人情報格納装置１０の指紋センサ１３Ａの上に所定の指を置いた状態で、情報機器本体３０の操作部３３から指紋登録を命令する。これにより、指紋登録命令が情報機器本体３０の制御部３１から制御ポート２４、読み出し／書き込み装置２０のインタフェース部２２を介して、可搬型個人情報格納装置１０へ送信される（ステップＳ２）。

指紋登録命令を受信した可搬型個人情報格納装置１０では、制御部１１により指紋認証部１３を制御して、指紋センサ１３Ａの上に置かれている指の指紋を読み取り、得られた指紋データをメモリ１３Ｂに書き込む（ステップＳ３）。これにより指紋登録が完了する。

【００１９】

次に、指紋登録がなされている可搬型個人情報格納装置１０に、事前にユーザＩＤおよび個人情報を格納するときの動作について、図６を参照して説明する。

予めユーザＩＤおよび個人情報を情報機器本体３０の記憶部３２に用意しておく。可搬型個人情報格納装置１０のコネクタ１６を読み出し／書き込み装置２０のコネクタ（図示せず）に差し込み、可搬型個人情報格納装置１０と読み出し／書き込み装置２０とが電気的に接続されると（ステップＳ１１，ＹＥＳ）、読み出し／書き込み装置２０から可搬型個人情報格納装置１０へ電力が供給される。

【００２０】

このとき、ユーザの指が可搬型個人情報格納装置１０の指紋センサ１３Ａに触れていれば（ステップＳ１２，ＹＥＳ）、制御部１１により指紋認証部１３を制御し、指紋照合を行う。具体的には、まず、指紋センサ１３Ａに触れているユーザの指紋を読み取る。その一

方で、メモリ１３Ｂから登録指紋データを読み出す。そして、ユーザの指紋データと登録指紋データとを照合回路１３Ｃにおいて照合する（ステップＳ１３）。その結果、２つの指紋データが一致すれば（ステップＳ１４，ＹＥＳ）、ユーザを登録者本人であると認証し、その旨を示す本人認証通知を制御部１１よりインタフェース部１４を介して読み出し／書き込み装置２０へ送信する（ステップＳ１５）。本人認証通知は、読み出し／書き込み装置２０のインタフェース部２２、制御ポート２４を介して、情報機器本体３０に入力される。

【００２１】

本人認証通知が入力された情報機器本体３０では、制御部３１の制御により記憶部３２からユーザＩＤおよび個人情報を読み出し、入出力ポート２３を介して読み出し／書き込み装置２０へ出力する。読み出し／書き込み装置２０では、入力されたユーザＩＤおよび個人情報を暗号化／復号化部２１において暗号化し（ステップＳ１６）、インタフェース部２２を介して可搬型個人情報格納装置１０へ送信する。可搬型個人情報格納装置１０では、インタフェース部１４を介して受信された暗号化されたユーザＩＤおよび個人情報を、制御部１１の制御によりメモリ１２に書き込む（ステップＳ１７）。これにより、可搬型個人情報格納装置１０へのユーザＩＤおよび個人情報の格納が完了する。

【００２２】

一方、指紋照合においてユーザの指紋データと登録指紋データとが一致しなければ（ステップＳ１４，ＮＯ）、ユーザを登録者本人であるとは認証できないので、可搬型個人情報格納装置１０の制御部１１よりエラーメッセージを読み出し／書き込み装置２０を介して情報機器本体３０へ送信する（ステップＳ１８）。情報機器本体３０では、制御部３１により表示部３４を制御してエラーが発生したことを表示し、個人情報を可搬型個人情報格納装置１０に書き込むことができなかったことをユーザに知らせる。

【００２３】

なお、ここでは指紋照合に際して可搬型個人情報格納装置１０の制御部１１が自立的にその制御を行う例を説明したが、情報機器本体３０の制御部３１より送信される指紋照合命令にしたがって可搬型個人情報格納装置１０において指紋照合を行うようにしてもよい。

【００２４】

次に、可搬型個人情報格納装置１０からユーザＩＤおよび個人情報を読み出すときの動作について、図７を参照して説明する。なお、可搬型個人情報格納装置１０には、すでに指紋登録がなされており、かつ、ユーザＩＤおよび個人情報が格納されているものとする。可搬型個人情報格納装置１０のコネクタ１６を読み出し／書き込み装置２０のコネクタ（図示せず）に差し込み、可搬型個人情報格納装置１０と読み出し／書き込み装置２０とが電気的に接続されると（ステップＳ２１，ＹＥＳ）、読み出し／書き込み装置２０から可搬型個人情報格納装置１０へ電力が供給される。

【００２５】

このとき、ユーザの指が可搬型個人情報格納装置１０の指紋センサ１３Ａに触れていれば（ステップＳ２２，ＹＥＳ）、制御部１１により指紋認証部１３を制御して、指紋照合を行う。具体的には、まず、指紋センサ１３Ａに触れているユーザの指紋を読み取る。その一方で、メモリ１３Ｂから登録指紋データを読み出す。そして、ユーザの指紋データと登録指紋データとを照合回路１３Ｃにおいて照合する（ステップＳ２３）。その結果、２つの指紋データが一致すれば（ステップＳ２４，ＹＥＳ）、ユーザを登録者本人であると認証する。すると、制御部１１の制御によりメモリ１２に格納されている暗号化されたユーザＩＤおよび個人情報を読み出し、インタフェース部１４を介して読み出し／書き込み装置２０へ送信する（ステップＳ２５）。

【００２６】

読み出し／書き込み装置２０では、インタフェース２２を介して受信された暗号化されたユーザＩＤおよび個人情報を、暗号化／復号化部２１において復号化して元のユーザＩＤおよび個人情報に戻し（ステップＳ２６）、入出力ポート２３を介して情報機器本体３０内の必要箇所へ送る。このように、本人認証が行われるとすぐに、ユーザＩＤおよび個人

情報が情報機器本体３０内の必要箇所へ送られる。

【００２７】

一方、指紋照合においてユーザの指紋データと登録指紋データとが一致しなければ（ステップＳ２４，ＮＯ）、ユーザが登録者本人であるとは認証できないので、可搬型個人情報格納装置１０の制御部１１よりエラーメッセージを読み出し／書き込み装置２０を介して情報機器本体３０へ送信する（ステップＳ２７）。情報機器本体３０では、制御部３１により表示部３４を制御してエラーが発生したことを表示し、個人情報を可搬型個人情報格納装置１０から読み出すことができなかったことをユーザに知らせる。

【００２８】

なお、ここでは指紋照合に際して、可搬型個人情報格納装置１０の制御部１１が自立的にその制御を行う例を説明したが、情報機器本体３０の制御部３１より送信される指紋照合命令にしたがって、可搬型個人情報格納装置１０において指紋照合を行うようにしてもよい。

また、ユーザＩＤおよび個人情報の読み出しに際して、可搬型個人情報格納装置１０の制御部１１が自立的にその制御を行う例を説明したが、本人認証後、可搬型個人情報格納装置１０の制御部１１より本人認証通知を送信し、これを受信した情報機器本体３０の制御部３１より送信される読み出し命令にしたがって、可搬型個人情報格納装置１０においてユーザＩＤおよび個人情報の読み出しを行うようにしてもよい。

【００２９】

以上のように、可搬型個人情報格納装置１０において指紋を用いた本人認証を行い、本人であると認証されたときに個人情報の読み出しまたは書き込みを行なうようにした。このため、ユーザが本人でない場合には読み出しまたは書き込みを行えないので、他人による成りすまし利用を未然に防止することができる。

また、可搬型個人情報格納装置１０に格納される個人情報を暗号化するようにしたので、たとえ可搬型個人情報格納装置１０が盗まれたとしても、格納されている個人情報が読み取られる可能性は小さい。その一方、可搬型個人情報格納装置１０を読み出し／書き込み装置２０に接続して利用する場合には、可搬型個人情報格納装置１０から暗号化された個人情報を読み出す際、これを読み出し／書き込み装置２０において復号化することにより、情報機器本体３０では暗号化前の個人情報を利用することができる。

【００３０】

なお、本実施の形態では、可搬型個人情報格納装置１０と読み出し／書き込み装置２０とをコネクタを介して接続する例を示したが、具体的にはＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）やＩＥＥＥ１３９４等のインタフェース技術を適用できる。また、このような有線インタフェース技術に限定されるわけではなく、Ｂｌｕｅｔｏｏｔｈ等の無線インタフェース技術や、ＩｒＤＡ等の赤外線インタフェース技術を利用してもよい。このように無線インタフェース技術等を利用することにより、コネクタ接続部分を探す手間が省け、一層使い勝手のよいシステムを実現できる。具体的には、非接触型のＩＣカードに指紋認証部１３を内蔵する例が挙げられる。

【００３１】

また、本実施の形態では、可搬型個人情報格納装置１０において本人認証を行うのに指紋を用いる例を示したが、指紋の代わりに本人と他人とを区別できる他の生体情報を用いて本人認証を行なうようにしてもよい。

また、本実施の形態では、読み出し／書き込み装置２０と情報機器本体３０とが別体である例を示したが、読み出し／書き込み装置２０の諸機能が当初から情報機器に組み込まれているものであってもよい。

【００３２】

また、図１には可搬型個人情報格納装置１０が制御部１１を有する例を示したが、図８に示す可搬型個人情報格納装置１１０のように制御部を有していなくてもよい。この場合、可搬型個人情報格納装置１１０の各部の制御は情報機器本体３０の制御部３１によって直接行われる。例えば、指紋認証部１３における指紋照合や、メモリ１２からのユーザＩＤ

および個人情報の読み出しが、情報機器本体３０からの命令に基づいて行われる。

【００３３】

【発明の効果】

以上説明したように、本発明では、ユーザから取得した指紋データと予め登録されている指紋データとが一致した場合にユーザを登録者本人であると認証し、登録者本人であると認証されたときに記憶手段に対する個人情報の読み出しまたは書き込みを行なうようにした。このため、ユーザが指紋データの登録者でない場合には、読み出しまたは書き込みを行えないので、他人による成りすまし利用を未然に防止することができる。

【００３４】

また、本発明では、記憶手段に書き込まれる個人情報を暗号化手段で暗号化することにより、たとえ個人情報格納装置が盗まれたとしても、記憶手段の内容が読み取られる可能性が小さくなる。その一方、個人情報格納装置を読み出し／書き込み装置に接続して利用する場合には、記憶手段から暗号化された個人情報を読み出す際、これを復号化手段で復号化することにより、情報機器本体では暗号化前の個人情報を利用することができる。

【００３５】

したがって、本発明によれば、個人情報格納装置で安全かつ確実に個人情報を保持し、その個人情報を目的の情報機器で利用できるようになる。

【図面の簡単な説明】

【図１】本発明の一実施の形態に係る個人情報入出力システムの全体構成を示すブロック図である。

【図２】可搬型個人情報格納装置の指紋認証部の構成を示すブロック図である。

【図３】可搬型個人情報格納装置の外観を示す図である。

【図４】個人情報入出力システムの使用イメージを示す図である。

【図５】可搬型個人情報格納装置に指紋登録をするときの動作の流れを示すフローチャートである。

【図６】可搬型個人情報格納装置にユーザＩＤおよび個人情報を格納するときの動作の流れを示す図である。

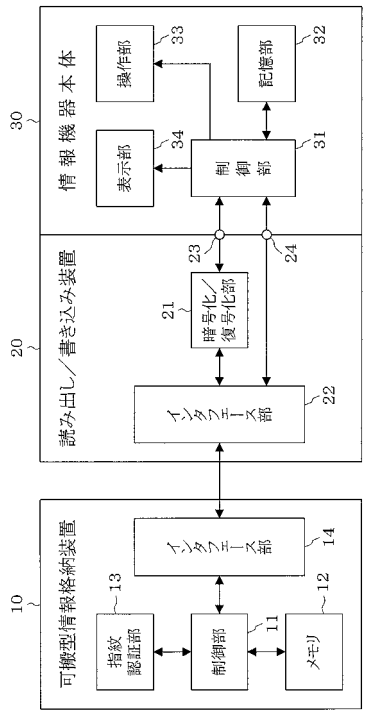
【図７】可搬型個人情報格納装置からユーザＩＤおよび個人情報を読み出すときの動作の流れを示す図である。

【図８】本発明の他の実施の形態に係る個人情報入出力システムの全体構成を示すブロック図である。

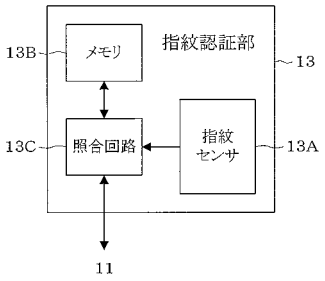
【符号の説明】

１０，１１０…可搬型個人情報格納装置、１１…制御部、１２…メモリ、１３…指紋認証部、１３Ａ…指紋センサ、１３Ｂ…メモリ、１３Ｃ…照合回路、１４…インタフェース部、１５…ケース、１６…コネクタ、２０…読み出し／書き込み装置、２１…暗号化／復号化部、２２…インタフェース部、２３…入出力ポート、２４…制御ポート、３０…情報機器本体、３１…制御部、３２…記憶部、３３…操作部、３４…表示部。

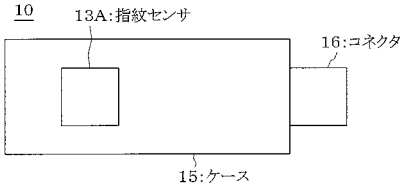
【図１】


情報機器本体
30
操作部
33
表示部
34
制御部
31
記憶部
32
読み出し／書き込み装置
20
23
24
暗号化／復号化部
21
インタフェース部
22
可搬型情報格納装置
10
インタフェース部
14
指紋認証部
13
制御部
11
メモリ
12

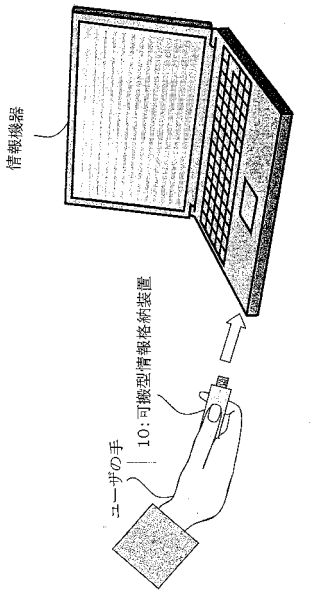
【図２】


13B
メモリ
指紋認証部
13
13C
照合回路
指紋センサ
13A
11

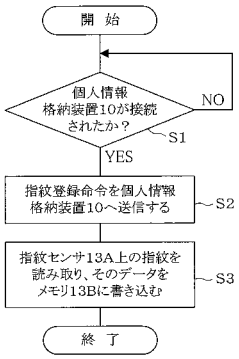
【図３】


10
13A:指紋センサ
16:コネクタ
15:ケース

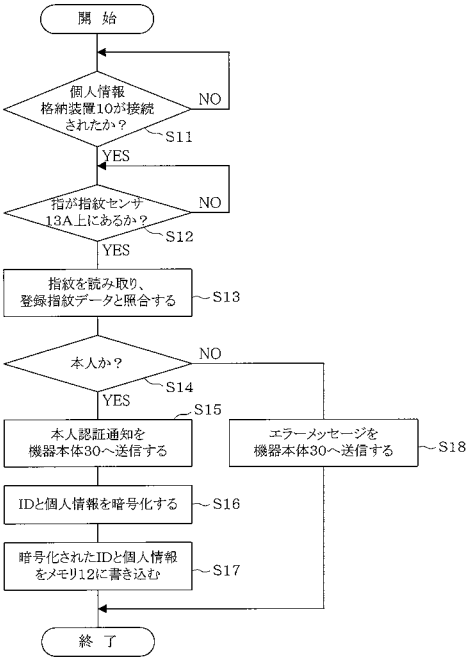
【図４】


情報機器
10:可搬型情報格納装置
ユーザの手

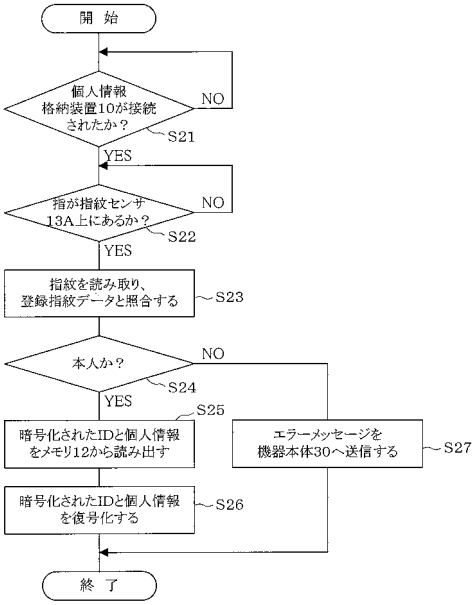
【図５】


開始
個人情報格納装置10が接続されたか？
NO
S1
YES
指紋登録命令を個人情報格納装置10へ送信する
S2
指紋センサ13A上の指紋を読み取り、そのデータをメモリ13Bに書き込む
S3
終了

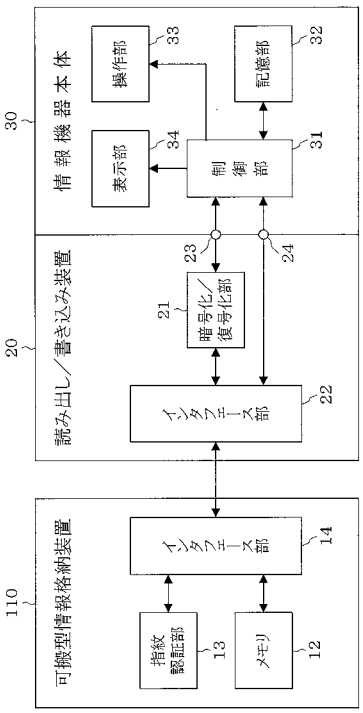
【図６】


開 始
個人情報
格納装置10が接続
されたか？
NO
S11
YES
指が指紋センサ
13A上にあるか？
NO
S12
YES
指紋を読み取り、
登録指紋データと照合する
S13
本人か？
NO
S14
YES
S15
本人認証通知を
機器本体30へ送信する
エラーメッセージを
機器本体30へ送信する
S18
IDと個人情報を暗号化する
S16
暗号化されたIDと個人情報
をメモリ12に書き込む
S17
終 了

【図７】


開 始
個人情報
格納装置10が接続
されたか？
NO
S21
YES
指が指紋センサ
13A上にあるか？
NO
S22
YES
指紋を読み取り、
登録指紋データと照合する
S23
本人か？
NO
S24
YES
S25
暗号化されたIDと個人情報
をメモリ12から読み出す
エラーメッセージを
機器本体30へ送信する
S27
暗号化されたIDと個人情報
を復号化する
S26
終 了

【図８】


30
情報機器本体
操作部
33
記憶部
32
表示部
34
制御部
31
23
24
20
読み出し／書き込み装置
21
暗号化／復号化部
インタフェース部
22
110
可搬型情報格納装置
インタフェース部
14
指紋認証部
13
メモリ
12

フロントページの続き

(51)Int.Cl.[7]	FI	テーマコード（参考）
	Ｇ０６Ｋ 19/00 Ｓ	

Ｆターム(参考) 5B085 AA08 AE23 AE25 AE26 AE29 BG02 BG04 BG07
5J104 KA01 KA17 NA38 NA41